

UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person, by name and address)*

16 Colonial Pines Circle, Pinehurst, NC 28374

Case No. 1:20MJ365-1

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Middle District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 USC § 875(c)

Transmit in Interstate
Person

Offense Description

Commerce a Communication Containing a Threat to Injure a

The application is based on these facts:

☒ Continued on the attached sheet.


☐ Delayed notice of _____ days *(give exact ending date if more than 30 days)* _____ is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

*Richard B. Starnes**Applicant's signature*

RICHARD B. STARNES, TFA, SPECIAL AGENT, FBI-JTTF

Printed name and title

On this day, the applicant appeared before me via reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.

Date: 12/14/2020 1:26pmCity and state: Durham, North Carolina*Judge's signature*

Honorable Joe L. Webster, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH
OF THE PREMISES LOCATED AT
16 Colonial Pines Circle, Pinehurst,
NC 28374

Case No.: 1:20MJ365-1

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Richard B. Starnes, being first duly sworn, hereby depose and state that the following is true to the best of my information, knowledge and belief:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for the premises 16 Colonial Pines Circle, Pinehurst, NC 28374 (SUBJECT PREMISES), to seize evidence described in Attachment A, and to search any seized evidence for items that constitute the commission of, contraband, the fruits of crime, or instrumentalities of violations of Title 18, United States Code, 875(c), Transmit in Interstate Commerce a Communication Containing a Threat to Injure a Person.

2. 1. I am a duly appointed Special Agent ("SA") U.S. Army Criminal Investigation Command ("USACIDC") and have been so employed since April 2015. I am currently assigned as a Task Force Agent with the FBI Joint Terrorism Task Force. As a Special Agent of USACIDC and TFA for the FBI, I am authorized to investigate crimes involving all violations of the Uniform Code of Military Justice,

and other applicable federal and state laws where there is an Army interest. Your affiant is currently assigned to the Charlotte Division, Fayetteville Resident Agency, Fayetteville, NC. Your affiant is primarily assigned to investigate matters involving domestic terrorism, including those laws relating to the federal violation below. Your affiant has conducted, as well as assisted other law enforcement officers, with physical surveillance, search warrants, and arrests of persons involved in a spectrum of federal violations. I have successfully completed the U.S. Army Criminal Investigation Division's Special Agent Course located at the U.S. Army Military Police School, Fort Leonard Wood, MO, which is a federally accredited criminal investigator training program. During my training at the Special Agent Course, I received legal instruction and advanced formal training on a variety of criminal investigations, including the use of the U.S. Army Criminal Investigation Division and FBI in furtherance of criminal activity such as identity theft, mail fraud, bank fraud, extortion, child pornography and other related offenses. I have completed the Network Intrusion Basics Course, Introduction to Networks and Hardware, Computer Incident Response Course, and the Windows Forensic Examiner Course through the Defense Cyber Investigations Training Academy ("DCITA"). I have also completed the Digital Evidence Acquisition Specialist Program and the Vehicle Data Extraction Training Program, which are federally accredited training programs located at the U.S. Federal Law Enforcement Training Center. Additionally, I have completed CID Special Agent courses that include the Special Victims Training Program, the Criminal Intelligence Training Program,

Hostage/Crisis Negotiator Level One Training Course, the U.S. Army Special Forces Technical Exploitation Course, and the BATF Level One Post-Blast Investigation Course. Prior to my position with the FBI, I was employed as a Special Agent with U.S. Army CID as a cyber investigator. Additionally, and prior to working for U.S. Army CID, I was employed as a Police Officer with the Charlotte-Mecklenburg Police Department for approximately thirteen years where I obtained my basic and advanced law enforcement certificates for the State of North Carolina. My duties as an officer included the investigation and enforcement of criminal laws in the State of North Carolina. Additionally, I served as a U.S. Army Reserve CID Special Agent from 2009 to 2019 where I retired from military service. My duties as a reserve U.S. Army CID Special Agent included investigating general crimes (to include but not limited to murder, sexual assaults, various forms of fraud and related offenses) as well as conducting technical sensitive site exploitation in the war on terror. I hold an A.A.S. in Logistics from the Community College of the Air Force, a B.A. in Criminal Justice from UNC-Charlotte, a B.S. in Emergency Management from Western Carolina University, a M.S. in Security Studies from East Carolina University, a Master's Executive Certificate in Negotiations from the University of Notre Dame and currently pursuing a Doctorate of Strategic Leadership from Regent University.

3. I make this affidavit in support of a search warrant for the SUBJECT PREMISES. I also make this affidavit in support of a search warrant for the person known as Theodore Macon CARRINGTON, Jr., for evidence of violations of Title 18,

United States Code, Section 875(c), Transmit in Interstate Commerce a Communication Containing a Threat to Injure a Person.

4. The facts in this affidavit come from my own personal observations, my training experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

5. Since this affidavit is being submitted for the limited purpose of securing a search and seizure warrant, I have not included each and every fact known to me concerning this investigation. I have set forth the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of Title 18, United States Code, Sections 875(c) are located in the place described in Attachment A.

RELEVANT STATUTES

6. Title 18 United States Code, Section 875(c) states: Whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both.

DEFINITIONS

7. The following definitions apply to this Affidavit and Attachment B:

- a. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."
- b. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, mobile telephones, video gaming devices, portable electronic music players, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).
- c. "Digital Device," as used herein, is defined as any electronic device capable of processing and/or storing data in digital form, including, but

not limited to: central processing units, laptop or notebook computers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, cables and connections, electronic storage media, electronic/digital security devices, and wireless communication devices such as telephone paging devices, beepers, mobile or cellular telephones, "smart" watches, personal data assistants ("PDAs"), iPods, BlackBerrys, digital cameras and digital gaming devices.

- d. "Downloading," is the process of transferring a file from the Internet and saving it as a file in one's computer hard drive.
- e. "Uploading," is the process of transferring a file from one's computer to the computer of another user via the Internet.
- f. "Hashing," is a powerful and pervasive technique used in nearly every examination of seized digital media. The concept behind hashing is quite elegant: take a large amount of data, such as a file or all the bits on a hard drive and use a complex mathematical algorithm to generate a relatively compact numerical identifier (the hash value) unique to that data. Examiners use hash values throughout the forensics process, from acquiring the data, through analysis, and even into legal proceedings. Hash algorithms are used to confirm that when a copy of

data is made (commonly referred to as a forensically sound image, the original is unaltered and the copy is identical, bit-for-bit." A hash value can be thought of as a digital fingerprint of the information.

- g. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as CD-ROMs, digital video disks (DVDs), Multi Media Cards (MMCs), memory sticks, smart cards, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).
- h. A "storage medium" is any physical object upon which computer data can be recorded. Examples include CD-ROMs, DVDs, and other magnetic or optical media.

- i. E-mail and web hosting companies, such as Microsoft, provide e-mail, webhosting, and other services to the public. Microsoft maintains computers that are connected to the Internet, and their subscriber/customers use those computers to, among other things, send and receive e-mail and operate websites that are available to others browsing the World Wide Web.
- j. E-mail providers' customers place files, software code, databases, and other data on the servers. To do this, customers connect from their own computers to the server computers across the Internet. This connection can occur in several ways. In some situations, it is possible for a customer to upload files using a special web site interface offered by the web hosting company. It is frequently also possible for the customer to directly access the server computer through the Secure Shell ("SSH") or Telnet protocols. These protocols allow remote users to type commands to the web server. The SSH protocol can also be used to copy files to the server. Customers can also upload files through a different protocol, known as File Transfer Protocol ("FTP"). Servers often maintain logs of SSH, Telnet, and FTP connections, showing the dates and times of the connections, the method of connecting, and the Internet Protocol addresses ("IP addresses") of the remote users' computers (IP addresses are used to identify computers connected to the Internet). Servers also commonly log the port number associated with the connection. Port numbers assist computers in determining how to interpret incoming and outgoing data. For example, SSH, Telnet, and FTP are generally assigned to different ports.
- k. Web sites deliver their content to users through the Hypertext Transfer Protocol ("HTTP"). Every request for a page, image file, or other resource is made through

an HTTP request between the client and the server. The server sometimes keeps a log of all of these HTTP requests that shows the client's IP address, the file or resource requested, the date and time of the request, and other related information, such as the type of Web browser the client uses.

1. In some cases, a subscriber or user will communicate directly with an e-mail provider about issues relating to an e-mail account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the company's support services, as well records of any actions taken by the company or user as a result of the communications.

PROBABLE CAUSE

8. This affidavit is submitted in support of a search warrant involving Theodore Macon CARRINGTON, Jr. who knowingly and willfully transmitting in interstate commerce a communication containing a threat to injure a person in violation of Title 18 United States Code Section 875(c).

9. The information contained in this affidavit is based on my knowledge of the facts and evidence obtained during the FBI's investigation of Mr. CARRINGTON and comes from my personal observations, my training and experience, and information obtained from other law enforcement agents and witnesses. Since this affidavit is being submitted for the purpose of establishing probable cause for the issuance of an arrest warrant, I have not included each and

every fact known to me concerning this investigation and have set forth only those facts I believe are necessary for said purpose.

10. On November 10th, 2020, LT. Lee Gatling, Pinehurst Police Department contacted the FBI Fayetteville RA about an email associated with Theodore CARRINGTON, Jr. posting a threat to kill U.S. Senator Ron Johnson.

11. Separately, United States Senator Ron Johnson's office notified the FBI Washington Field Office of the same email. The email was sent to Senator Johnson's whistleblower email address.

12. LT. Gatling gave the following background on CARRINGTON: Theodore Macon CARRINGTON has continuously implicated Pinehurst Police Department personnel, along with additional entities (local, state, and federal), in alleged narcotics trafficking, pedophilia, and extortion. CARRINGTON harasses public officials via emails and has consistently posted blogs with Pinehurst Police Department officers' names in the blogs and YouTube videos while using hostile verbiage. This has been an ongoing issue since 2009. CARRINGTON has a lengthy criminal history and significant law enforcement involvements to including charged offenses both Federally and in North Carolina State Courts for assault, damage to property, resisting a public officer, threatening an Executive Legal Court Officer, and for threatening to kill the President of the United States (President Obama in 2009).

13. Based on information provided during canvass of the neighbors and confirmation from the Pinehurst Police Department's records of multiple calls for service to the address, it has been determined that CARRINGTON resides at 16 Colonial Pines Circle, Pinehurst, NC 28374 with his mother. On November 11th, 2020, your affiant spoke to the neighbor of CARRINGTON who stated he last saw CARRINGTON at the above address two days prior on November 9th, 2020. The threatening email was sent by CARRINGTON on November 6th, 2020.

14. On Friday, November 6th, 2020, an email was sent from email address theodore231@outlook.com, which is associated with Theodore CARRINGTON. The email was sent to Senator Ron Johnson via his whistleblower email address as well as multiple other email addresses. The subject of the email was titled: "TO Senator Ron Johnson – I'll Fucking Kill You Dead".

15. The main body of the email contained the following: "Motherfucker, Me and my Mom are being Poisined (sic) and Smartmetered (sic) in Pinehurst NC. The PIGS in Alabama and the FBI win't (sic) let us move out of our house in Pinehurst, which is a Kill BOX. Why the HELL do you have a Whistle Blower Email Drop? If it is the Last thing I do, I'm coming to Kill You. Macon CARRINGTON".

16. On December 1st, 2020 On December 1st, 2020, Theodore Macon CARRINGTON Jr, 08/04/1966 (DOB), was interviewed at the Guest House Inn located at 110 Frontage Road Aiken, South Carolina 29801. After being advised of

the identity of the interviewing Special Agent (SA) and Task Force Officer (TFO) and the nature of the interview, CARRINGTON provided the following information:

17. CARRINGTON was advised he was not under arrest. CARRINGTON agreed to speak with your affiant.

18. CARRINGTON stated he was upset because he contacted U.S. Senator Johnson over a period of time and told him he was being poisoned and was being hit in the head with an electric ray gun. CARRINGTON kept giving the Senator information on things going on and the U.S. Senator did absolutely nothing while CARRINGTON was almost being killed in Pinehurst, North Carolina. Upon request by the undersigned, Senator Johnson's office indicated they had no prior record of communications from CARRINGTON on the topics he described.

19. Your affiant asked CARRINGTON if he sent an email to Senator Johnson stating he was going to kill him to which CARRINGTON responded, "I'll own it, I did it". CARRINGTON stated he was angry because the Senator had not replied to his correspondence.

20. CARRINGTON stated he would talk to other law enforcement and provided his email address and phone number. CARRINGTON wrote the information on a Pall Mall 100's cigarette package (on a torn piece of the package) displaying theodore231@outlook.com and telephone number 505-302-4548.

21. Your affiant received information generated by the United States Secret Service that on December 4th, 2020 an email originating from theodore231@outlook.com was sent to the RAND Corporation, The Washington Post,

educational institutions (including Wake Forest University, located in Winston-Salem, North Carolina), and the US Army that included references to numerous USSS protectees and government officials. In the email, CARRINGTON claimed he was recovering in an Aiken, SC, hotel after being poisoned and targeted with a "microwave weapon." He wrote that he was involved in the "Deep State War" and worked with "a bunch of Underworld CIA types" who "jack" corporations, the Army, politicians, lawyers cops, and judges. CARRINGTON further alleged "we're taking out Trump, Biden, Chris Wray, Bushs, Clintons, EVERYBODY – By Christmas."

22. The FBI Washington Field Office reported to your affiant that on December 7th, 2020, an email originating from theodore231@outlook.com was sent to Senator Mitch McConnell (and multiple other email addresses) with a threat to Senator McConnell's life. The email stated "I've had it with you and your God Damned Confucious Spy Ring Mothetrucker. I just put a Hit on You and Elaine. And you can't have me arrested, or do Jack Shit. That ought to Worry You. I am Coming to Murder You. Now try and Fucking do Something About It. Macon CARRINGTON." Senator McConnell's office notified the FBI upon receipt.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

23. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

24. There is probable cause to believe that things that were once stored on the device may still be stored there. The following facts support my assertion of probable cause:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear, rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic

evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

25. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the digital device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the digital devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave

traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to

investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

26. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the forensic images consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

27. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

28. *Manner of execution.* In light of these concerns, I hereby request permission to seize any records, electronic storage mediums, and computer hardware (including associated peripheral USB digital devices which were imaged with consent) that are believed to contain some or all of the evidence described in the authorization, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the computer hardware on-site for this evidence.

29. Searching computer systems for the evidence described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the authorization. Criminals can mislabel or hide files and directories, encode communications to avoid using key words, attempt to delete files to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require agents and law enforcement or other analysts with appropriate expertise to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files or peruse every file briefly to determine whether it falls within the scope of the authorization. In light of these difficulties, FBI intends to use whatever data

analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B.

REQUEST FOR SEALING OF APPLICATION/AFFIDAVIT

30. It is respectfully requested that this Court issue an order sealing, until further order of this Court, all papers submitted in support of this Application, including the Application, Affidavit, and Search Warrant, and the requisite inventory notice (with the exception of one copy of the warrant and the inventory notice that will be left at the SUBJECT PREMISES). Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation and not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through forums. Premature disclosure of the contents of this Affidavit and related documents may have a significant and negative impact on this continuing investigation and may jeopardize its effectiveness by alerting potential targets to the existence and nature of the investigation, thereby giving them an opportunity to flee, or to destroy or tamper with evidence.

CONCLUSION

31. I submit that this affidavit supports probable cause for a search warrant to search the SUBJECT PREMISES described in Attachment A for the

things described therein and a subsequent search of the seized items for records and information set out in Attachment B which are related to the offense also set out there, and seizure of those records and information.

32. Based on the foregoing, your affiant respectfully asserts that there is probable cause to believe CARRINGTON transmitted a threat in interstate commerce to injure the person of another, in violation of Title 18, United States Code, Section 875(c).

FURTHER AFFIANT SAYETH NAUGHT.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Respectfully submitted,

Richard B. Starnes

Richard B. Starnes
Special Agent
TFA- Federal Bureau of Investigation

In accordance with Rule 4.1(b)(2)(A), the Affiant attested under oath to the contents of this Affidavit, which was submitted to me by reliable electronic means, on this 14th day of December, 2020, at 1:26p.m.



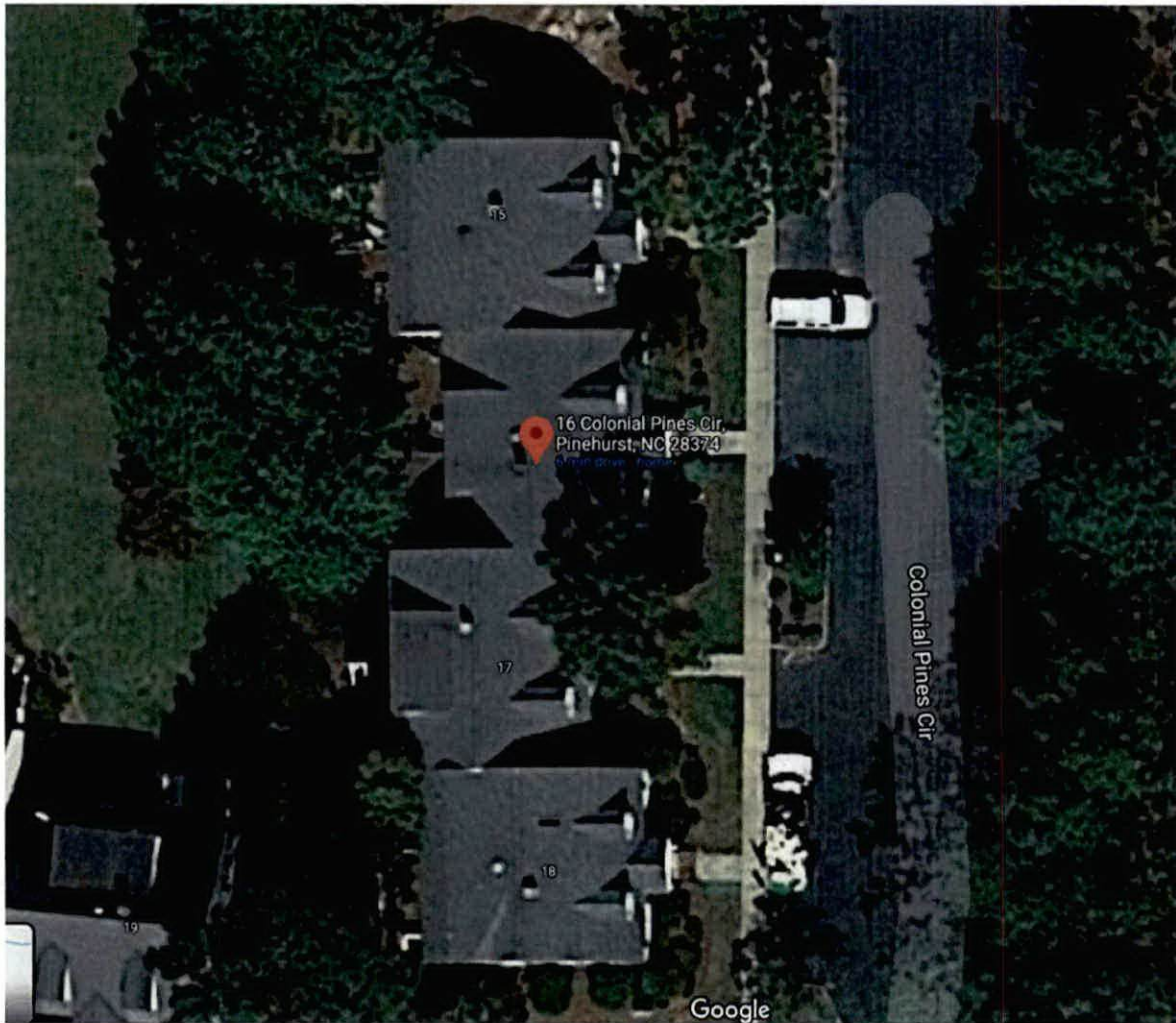
HONORABLE JOE L. WEBSTER
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

PREMISES TO BE SEARCHED

The premises to be searched is the entire premises located at 16 Colonial Pines Circle, Pinehurst, NC 28374, hereinafter the SUBJECT PREMISES. The SUBJECT PREMISES is more fully described as a two-story townhouse. The townhouse is light green in color with a white front door. There is a see-through glass storm door preceding the front door. The front door's door handle is located on the left side of the door and opens inward. The storm door's handle is also on the left and opens towards the outside of the residence. As of December 14th, 2020, there is a green wreath on the front door adorned with a red bow. The rear door is accessible via a small wooden deck with six steps leading to the top of the deck. The rear doors appear to be French doors with approximately fifteen glass panels in each door. Due to the ability and ease for individuals to upload and save electronic communications onto media storage devices such as CDs, DVDs, and thumb drives, which can be easily concealed and stored inside of a vehicle, the premises to be searched includes vehicles owned and/or operated by Theodore Macon CARRINGTON, Jr., resident/occupant of the SUBJECT PREMISES. The subject has been driving a 2007 Hyundai Tucson displaying North Carolina registration HJS-5555 and VIN# KM8JN12D87U619634. As of December 14th, 2020, the vehicle's registration plate has been removed from the vehicle.

A birds-eye view photograph of the SUBJECT PREMISES is below:



***Photo retrieved from Google Maps**

Photographs of the SUBJECT PREMISES' exterior (front of building/entrance to residence) are below:



*Photo retrieved from Zillow.com. Photos affirmed to be correct based on surveillance. Unable to obtain current photos due to open windows and the potential for subject to see photos being taken from within the residence.

Photographs of the SUBJECT PREMISES' exterior (rear of building/entrance to residence) are below:



*Photo retrieved from Zillow.com. Photos affirmed to be correct based on surveillance. Unable to obtain current photos due to open windows and the potential for subject to see photos being taken from within the residence.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED

Contraband, fruits, instrumentalities, and evidence of violations of Title 18, United States Code, Section 875(c) (activities relating to interstate communication of threats), including:

1. Information, correspondence, records, documents or other materials, including computers, mobile phones, or storage media, constituting evidence of or pertaining to the transmission of threats of injury through interstate or foreign commerce
2. For any computer, mobile phone or storage medium whose seizure is authorized by this authorization, and any image of such computer, mobile phone or storage medium (hereinafter, "COMPUTER"):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this search and seizure authorization were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer," includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium," includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, DVDs, and other magnetic, electronic, or optical media.